Data Sheet

Cisco VPN 3000 Series Concentrators

The Cisco® VPN 3000 Series offers best-in-class remote-access VPN devices that provide businesses with unprecedented cost savings through flexible, reliable, and high-performance remote-access solutions. The Cisco VPN 3000 Series offers solutions for the most diverse remote-access deployments by offering both IP Security (IPsec) and Secure Sockets Layer (SSL)-based VPN connectivity on a single platform.

Corporations use VPNs to establish secure, end-to-end private network connections over a public networking infrastructure, allowing them to reduce their communications expenses. By offering both SSL and IPsec VPN on one platform—without the expense of special feature licensing—the Cisco VPN 3000 Series provides customers with cost-effective alternatives to deploying parallel remote-access infrastructures. Remote connections can be established either from a SSL-capable Web browser or from VPN client software, allowing for maximum flexibility and application access. This centralized architecture provides ease of management and implementation in deployments that require detailed access controls for numerous deployment scenarios with diverse user communities, including mobile workers, telecommuters, and extranet users.

FEATURES AND BENEFITS

To fully realize the benefits of high-performance, secure remote access, a robust, highly available VPN solution is needed. Cisco VPN 3000 Concentrator Software v4.7 incorporates the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture that enables corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access application requirements.

New features in Cisco VPN 3000 Concentrator Software v4.7 deliver extensive application access, best-in-market endpoint security, data integrity protection, leading infrastructure access, and network compliance validation controls.

Benefits of the Cisco VPN 3000 Series include:

- **Advanced endpoint security**—A primary component of Cisco VPN 3000 Concentrator Software v4.7 is the Cisco Secure Desktop, which offers pre-connection security posture assessment and seeks to minimize data such as cookies, browser history, temporary files, and downloaded content from being left behind after an SSL VPN session terminates. The Cisco Secure Desktop feature is combined with IPsec client-enabled Are-You-There (AYT) support for personal firewall verification, and with IPsec client-enabled Network Admission Control (NAC), an industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. Together, these three solutions form a powerful endpoint security package that increase protection of confidential data and helps to combat costly network attacks.
- **Broad application support for SSL VPN**—The Cisco VPN 3000 Series Concentrator platform offers extensive application support through its dynamically downloaded SSL VPN client, enabling network-layer connectivity to virtually any application. The Cisco VPN 3000 Series delivers truly clientless support for Citrix application access, allowing a low-overhead extension of the network resources to VPN users through a standard Web browser. Pure clientless and thin-client port forwarding options may be deployed for environments with limited application access requirements, such as extranets.
- **Ease of deployment with zero-touch remote endpoint management**—Integrated Web-based management on Cisco VPN 3000 Series Concentrators provides a simple interface to configure and monitor all remote-access users, providing ease of manageability across both IPsec and SSL VPN environments. Group-based management features allow administrators to design security policies

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

and authentication methods for each group, which is essential when extending network resources to non-corporate-managed users and endpoints. For remote-access and site-to-site VPNs, ease of deployment is critical when technical resources are not available for configuration at the remote site. The Cisco Easy VPN solution, consisting of Cisco Easy VPN Remote and Easy VPN Server, pushes security policies defined at the central site to remote VPN devices, helping to ensure that those connections have up-to-date policies in place before the connection is established, thereby offering flexibility, scalability, and ease of use for site-to-site and remote-access VPNs.

- **Comprehensive deployment scenario coverage**—IPsec and SSL are complementary technologies that address unique user access requirements; both are necessary in order for a company to meet the needs of a diverse user base. Cisco VPN 3000 Series Concentrators support both IPsec and SSL VPN, allowing businesses to choose the most appropriate technology for users accessing the network through different scenarios. This provides maximum flexibility and application access, all on one platform, alleviating the need to deploy and manage separate infrastructures.
- **Simple, low, per-user pricing**—The simple licensing structure of the concentrator platform (no added licenses for special features), combined with the consolidated technology platform, provides customers with unparalleled cost savings and competitive per-user pricing. Cisco VPN 3000 Series Concentrators can scale to meet the demands of businesses of any size. The platform's unique multidevice clustering capability allows any remote-access solution to scale, cost-effectively, as a business grows. The load-balancing features of the Cisco VPN 3000 Series help ensure that remote-access connectivity is distributed evenly across a concentrator cluster without user intervention, eliminating any single point of failure.

SSL VPN—Cisco Clientless SSL VPN

Using only a Web browser and its native SSL encryption, SSL VPNs provide remote access—without the requirement of preinstalled VPN client software—to network resources from almost any Internet-enabled location. The Cisco clientless SSL VPN feature on Cisco VPN 3000 Series Concentrators enables customers to access any application, including Webpages, file shares, e-mail, and client-server applications, via SSL-enabled sessions.

Customized Application Access for Employees, Partners, and Non-Company-Managed PCs

Cisco delivers clientless, thin-client, and SSL tunneling client access methods, enabling the appropriate level of application access based on the end-system deployment environment, such as employees, extranets, and non-company-managed devices. With the SSL VPN Client, Cisco delivers a lightweight, centrally configured, easy-to-support SSL VPN tunneling client that allows access to virtually any application. The SSL VPN Client is compatible with any SSL-enabled browser and dynamically pushed to the user in one of three methods—ActiveX, Java, or an .exe file. Thin-client access with Cisco SSL VPN is achieved through a port forwarding mechanism enabled by a small Java applet download. Port forwarding relays data requested by the port on the local machine to the corresponding application port on the network side—granting the user access to more applications and network resources than a Web browser offers. Clientless access allows users to connect in, with little requirements beyond a basic Web browser, and access Web servers or resources such as file shares and e-mail through Microsoft Outlook Web Access 2003.

Table 1 lists some of the features of the Cisco SSL VPN Client.

Table 1. Cisco SSL VPN Client: Broad Application Access Through a Network-Tunneling Client

Feature	Description
Universal Application Access	• Provides full client capabilities over SSL, including access to Cisco IP SoftPhone and voice over IP (VoIP) support, increasing remote-user productivity
Ease of Download and Installation	• Dynamic download and multiple delivery methods help ensure seamless download and distribution with Java, ActiveX, or .exe • Small download size helps ensure rapid delivery • No reboot required after installation
Increased Security	Client may be either removed at end of session or left permanently installed

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Zero-Touch Remote Administration	Central site configuration provides integration, with no administration on the remote client side needed

Supported operating systems: Microsoft Windows 2000 and Windows XP

Advanced Endpoint Security with the Cisco Secure Desktop Minimizes the Risk of Data Theft

SSL VPN deployments enable universal access from both secure and non-corporate-managed endpoints, as well as the ability to extend network resources to diverse user communities. With this extension of the network, the points for potential network security attacks also increase. Whether users are accessing the network from a corporate-managed PC, personal machine, or public terminal, the Cisco Secure Desktop seeks to minimize data leakage from the SSL session.

The Cisco Secure Desktop Host Integrity Verification feature performs pre-connection posture assessment to verify that the endpoint seeking access possesses the particular antivirus, firewall, and OS or service pack features required, and detects certain installed malware before granting access to the network. The Cisco Secure Desktop then creates a secure vault for session information by generating a virtual "sandbox", on the machine. During the session, information is encrypted and written to the Cisco Secure Desktop partition on the hard drive. At the close of the session, the secure vault is eradicated using a U.S. Department of Defense (DoD) sanitization algorithm. Session information, including cache files, history, cookies, file downloads, and passwords are encrypted in real time, reducing the risk that data is left behind. This feature is unique from many comparable cache cleaning products that attempt a post-session cleanup of tracked files. Similarly, the automatic timeout features of the Cisco Secure Desktop help ensure that session information is erased, whether or not the user takes the active role in terminating the session. The Cisco Secure Desktop can often run with guest permissions, providing advanced protection on endpoints regardless of Web settings, browser types, or system privileges.

Table 2 lists features of Cisco Secure Desktop.

Table 2. Cisco Secure Desktop: Comprehensive Security of Information from the Network to the Endpoint

Feature	Description
Available with Guest Permissions	Users accessing the network from remote machines may not have administrator privileges on all systems. Cisco Secure Desktop can often be installed with only guest permissions, helping to ensure delivery and installation on all systems.
Pre-Connection Posture Assessment	Host Integrity Verification checking detects the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access.
Comprehensive Session Protection	Additional protection is provided for all data associated with the session, including passwords, file downloads, history, cookies, and cache files. Session data is encrypted to the secure vault of the Cisco Secure Desktop.
End-of-Session Data Cleanup	Data in the secure vault is overwritten at the end of the session.
Keystroke Logger Detection	Performs an initial check for certain software-based keystroke logging software at the start of the session. If an anomalous program begins running inside the secure vault, after session initiation, the user is prompted to stop the suspicious activity.

Terminal Server Support for Citrix

Businesses are experiencing a growing need to provide remote access to corporate information—securely, reliably, immediately, and with increasing cost efficiency. To minimize costs while maximizing remote connectivity options, many businesses are centralizing their application management and distribution to allow access to internal computing resources through a terminal server architecture. For this reason, it is important that a robust remote-access solution support Citrix deployments with a simple, dependable, and easy-to-use protocol, while providing a local system-based experience for application use. Typical SSL solutions require either a software client or the existence of an applet download (Java or ActiveX) to access internal terminal server resources; this slows application initiation and creates potential access problems, due to software conflicts or browser settings. Cisco VPN 3000 Series Concentrators provide truly clientless Citrix support without relying on additional Java-based port forwarding mechanisms, delivering rapid and highly stable system access, regardless of browser or security settings.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Table 3 provides a list of features associated with Cisco VPN 3000 Series support for Citrix.

Table 3. Citrix Support: Enhanced Access to Internal Network Infrastructure Resources with Clientless Citrix Support

Feature	Description
Access to System Resources	Clientless access alleviates potential issues caused when incongruent browser or security settings prohibit the download of a client or applet
Swift Connectivity	Application initiation is instantaneous, with no additional software client or applet downloads required
Highly Stable Support	Client software conflicts with unmanaged machines or unfamiliar images are avoided with clientless access

IPsec VPN—Cisco Easy VPN and Auto-Upgradable Cisco IPsec VPN Client

IPsec VPNs offer the security and encryption features necessary to protect enterprise data, IP voice, and video traffic as it traverses the Internet. Because IPsec can be deployed across any IP network, it is an attractive option for customers needing VPN services and has become the de-facto standard in remote access.

Fast, Easy, and Scalable Deployment

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to Cisco VPN 3000 Series Concentrators. This thin-client design, IPsec-compliant implementation is licensed for an unlimited number of users. The Cisco IPsec VPN Client can be preconfigured for mass deployments; the initial logons require little user intervention. It may be automatically upgraded to newer client versions upon user connection, easing client version management on remotely deployed systems. Using Cisco Easy VPN, VPN access policies are created and stored centrally in the concentrator and pushed to the client when a connection is established. This helps ensure dynamically updated, zero-touch configuration of IPsec remote clients. Cisco Easy VPN Remote allows dynamic configuration of end-user policy, requiring less manual configuration by end users and field technicians—reducing errors and further service calls while providing centralized security policy management. The Cisco Easy VPN Server allows the concentrator to act a VPN gateway for site-to-site or remote-access VPNs, and pushes security policies defined at the central site to the remote VPN device, helping to ensure that those connections have up-to-date policies in place before the connection is established.

Cisco VPN 3002 Hardware Client

The Cisco VPN 3002 Hardware Client is a small hardware appliance that operates as a client in VPN environments. It combines the best features of a software client, including scalability and easy deployment, with the stability and independence of a hardware platform. By integrating Cisco Easy VPN with the Cisco VPN 3002 Hardware Client, customers can reduce the management complexity of VPN deployments and simplify remote-side administration.

Comprehensive Security Policy Compliance with NAC

NAC is an industrywide collaboration effort led by Cisco, established to help ensure that every endpoint complies with network security policies before being granted access. Cisco VPN 3000 Concentrator Software v4.7 is NAC-enabled for IPsec remote-access scenarios. NAC reduces the risk associated with extending network resources in remote-access scenarios by preventing vulnerable hosts from obtaining and retaining normal network access. The Cisco AYT feature enforces firewall policies for users connecting using the Cisco IPsec VPN Client. Administrators can configure the VPN to refuse endpoints that are in violation of the designated firewall policy. The Cisco IPsec VPN Client polls the firewall every 30 seconds to make sure it is still running. AYT checks for the Cisco Security Agent, Cisco Integrated Client Firewall, Network ICE BlackICE Defender, Sygate Personal Firewall, Sygate Personal Firewall Pro, Sygate Security Agent, Zone Labs ZoneAlarm, and Zone Labs ZoneAlarm Pro.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Table 4 lists features of NAC.

Table 4. Network Admission Control: Prevents Noncompliant Endpoints from Affecting Enterprise Resilience

Feature	Description
Uses Existing Threat Mitigation Infrastructure	Offers cost savings to customers by using existing network and antivirus infrastructures
Protects the Network with the Network	Uses a network-based approach with NAC-enabled network access points (like Cisco VPN 3000 Series Concentrators) to ensure every host device is interrogated for policy compliance

PRODUCT PLATFORM HIGHLIGHTS

Table 5 lists highlights of the Cisco VPN 3000 Series.

Table 5. Cisco VPN 3000 Series Highlights

Feature	Description
High-Performance Distributed Processing Architecture	• Cisco Scalable Encryption Processing (SEP) modules provide hardware-based encryption, helping to ensure consistent performance throughout the rated capacity (Cisco VPN 3020, 3030, 3060, and 3080 Concentrators). • Large-scale tunneling support is provided for SSL, IPsec, Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP)/IPsec connections
Scalability (Cisco VPN 3015, 3020, 3030, 3060, and 3080 Concentrators)	• Modular design (four expansion slots) provides investment protection, redundancy, and a simple upgrade path (Cisco VPN 3030 and 3060 Concentrators only). • System architecture is designed to supply consistent, high-availability performance. • All-digital design provides the highest reliability and 24-hour continuous operation. • Robust instrumentation package provides run-time monitoring and alerts. • Microsoft compatibility offers large-scale client deployment and smooth integration with related systems. • Integrated device clustering (load-balancing) technology.
Security	• Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products. • Firewall capabilities through stateless packet filtering and address translation help ensure the required security of a corporate LAN. • User- and group-level management offer maximum flexibility; clientless SSL VPN offers granular access control per group and detailed logging information.
High Availability	• Redundant subsystems and multichassis failover capabilities help ensure maximum system uptime. • Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early warning alerts.
Robust Management	• Concentrators can be managed using any standard Web browser (HTTP or HTTPS) or using Telnet, SSHv1, and using a console port. Files can be accessed through HTTPS, FTP, and Secure Copy Protocol (SCP). • Configuration and monitoring capabilities are provided for enterprises and service providers. • Access levels are configurable by users and groups, allowing easy configuration and maintenance of security policies. For larger deployments, Cisco VPN 3000 Series Concentrators are supported in several Cisco network management applications, including: - Cisco IP Solution Center (ISC): Provisions site-to-site and remote-access VPN services - CiscoWorks Monitoring Center for Performance: Monitors and reports on remote-access and site-to-site VPN tunnel connections - CiscoWorks Resource Manager Essentials (RME): Provides operational management features such as software distribution, syslog reporting, and inventory management - CiscoWorks CiscoView: Provides real-time system status monitoring

SIX MODELS

The Cisco VPN 3000 Series offers six concentrator models. Each model supports the full suite of IPsec and SSL VPN.

Cisco VPN 3005 Concentrator

The Cisco VPN 3005 Concentrator is designed for small to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance), with support for up to 200 simultaneous IPsec sessions or 50 simultaneous clientless sessions. Encryption processing is performed in software. The Cisco VPN 3005 does not have built-in upgrade capability.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco VPN 3015 Concentrator

The Cisco VPN 3015 Concentrator is designed for small to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance), with support for up to 100 simultaneous IPsec sessions or 75 simultaneous clientless sessions. Like the Cisco VPN 3005, encryption processing is performed in software, but the Cisco VPN 3015 is also field-upgradable to the Cisco VPN 3030 and 3060 models.

Cisco VPN 3020 Concentrator

The Cisco VPN 3020 Concentrator is designed for medium-sized and large organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps maximum performance), with support for up to 750 simultaneous IPsec sessions or 200 simultaneous clientless sessions. Specialized SEP modules (SEP-E) perform hardware-based acceleration. The Cisco VPN 3020 cannot be upgraded to other products in the series. Redundant and nonredundant configurations are available.

Cisco VPN 3030 Concentrator

The Cisco VPN 3030 Concentrator is designed for medium-sized and large organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps maximum performance), with support for up to 1500 simultaneous IPsec sessions or 500 simultaneous clientless sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 can be upgraded to the Cisco VPN 3060 in the field. Redundant and nonredundant configurations are available.

Cisco VPN 3060 Concentrator

The Cisco VPN 3060 Concentrator is designed for large organizations that demand the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance), with support for up to 5000 simultaneous IPsec sessions or 500 simultaneous clientless sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and nonredundant configurations are available.

Cisco VPN 3080 Concentrator

The Cisco VPN 3080 Concentrator is optimized to support large enterprise organizations that demand the highest level of performance, combined with support for up to 10,000 simultaneous IPsec sessions or 500 simultaneous clientless sessions. Specialized SEP modules perform hardware-based acceleration. The VPN 3080 is available in a fully redundant configuration only.

MODEL COMPARISON

Table 6 provides a comparison of the Cisco VPN 3000 Series Concentrator models.

Table 6. The Cisco VPN 3000 Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3020	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous IPsec Users*	200	100	750	1500	5000	10,000
Simultaneous SSL VPN (Clientless) Users**	50	75	200	500	500	500
Maximum LAN-to-LAN Sessions	100	100	250	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware	Hardware
Available Expansion Slots	0	4	1 (redundancy option)	3 (redundancy option)	2 (redundancy option)	0 (fully redundant)
Encryption Module (SEP)	0	0	1	1	2	4
Redundant SEP	–	–	Optional	Optional	Optional	Yes
System Memory	32/64 MB (fixed)	128 MB	256 MB	512 MB	512 MB	512 MB

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Hardware Configuration	1U	Scalable 2U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Optional	Optional	Optional	Optional	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

*Assumes maximum device memory and SEP-E modules (Cisco VPN 3020, 3030, 3060, and 3080 models). For planning purposes, a simultaneous IPsec user is considered to be a remote-access VPN user connected in all-tunneling mode; this includes one IKE security association and two unidirectional IPsec security associations. Network sizing should take into consideration number of sessions, throughput per user, and aggregate throughput of the remote-access environment when choosing the appropriate Cisco VPN 3000 Series Concentrator model.

**Assumes maximum device memory and SEP-E modules (Cisco VPN 3020, 3030, 3060, and 3080 models). For planning purposes, a simultaneous SSL VPN user is considered to be a clientless VPN user retrieving a Webpage at up to every 60 seconds. Users log in at the rate of one per second and pass data for the duration of the test. The average retrieval time for the Webpage is less than or equal to five seconds.

TECHNICAL SPECIFICATIONS

Hardware	
Processor	Motorola PowerPC processor
Memory	• Redundant system images (Flash) • Variable memory options (Figure 6)
Encryption	• Cisco VPN 3005, 3015: Software • Cisco VPN 3020, 3030, 3060, and 3080: Hardware
Embedded LAN Interfaces	• Cisco VPN 3005: Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted) • Cisco VPN 3015, 3020, 3030, 3060, and 3080: Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted, and DMZ)
Instrumentation	• Cisco VPN 3005: Unit status indicator (front panel); status LEDs for Ethernet ports (rear panel) • Cisco VPN 3015, 3020, 3030, 3060, and 3080: Status LEDs for system, expansion modules, power supplies, Ethernet modules, and fan (front panel); status LEDs for Ethernet modules, expansion modules, and power supplies (rear panel) • Cisco VPN 3015, 3020, 3030, 3060, and 3080: Activity monitor displays the number of sessions, aggregate throughput, or CPU utilization, and is push-button selectable
Software	
Client Software Compatibility	• Cisco SSL VPN Client for network-layer connectivity using an SSL-capable Web browser on remote system • Cisco IPsec VPN Client for Windows 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSparc 32- and 64-bit); and Mac OS X 10.2, 10.3, and 10.4, including centralized split-tunneling control and data compression • Microsoft PPTP, Microsoft Point-to-Point Encryption (MPPE), and Microsoft Point-to-Point Compression (MPPC); Microsoft Challenge Handshake Authentication Protocol (MSCHAP) v1 and v2; and Extensible Authentication Protocol (EAP) and RADIUS passthrough for EAP-Transport Layer Security (EAP-TLS) and EAP-Generic Token Card (EAP-GTC) support • Microsoft L2TP and IPsec for Windows 2000 and XP, including Windows XP Dynamic Host Control Protocol (DHCP) option for route population • Microsoft L2TP and IPsec for Windows 98, ME, and NT Workstation 4.0
Tunneling Protocols	• Cisco SSL VPN (HTTPS/SSL-based) • IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with autodetection and fragmentation avoidance), IPsec/TCP • Support for Cisco EasyVPN (client and network extension mode)
Encryption/Authentication	• IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128/192/256-bit) with Message Digest Algorithm 5 (MD5) or Secure Hashing Algorithm (SHA); or MPPE using 40/128-bit RC4
Key Management	• Internet Key Exchange (IKE) • Diffie-Hellman (DH) groups 1, 2, 5, and 7 (ECDH) • RSA certificates (SSL and IPsec)
Routing	• Routing Initiation Protocol (RIP), RIPv2, Open Shortest Path First (OSPF), Reverse Route Injection (RRI), static routing, automatic endpoint discovery, NAT, and Classless Interdomain Routing (CIDR) • IPsec fragmentation policy control, including support for Path Maximum Transmission Unit (MTU) Discovery (PMTUD) • Interface MTU control
Third-Party Compatibility	iPass Ready, Funk Steel-Belted RADIUS, Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, and SA Keon
High Availability	• Virtual Router Redundancy Protocol (VRRP) for multichassis redundancy and multichassis failover • Remote-access load-balancing clusters supporting both SSL and IPsec connections • Destination pooling for client-based failover, re-establishment, and connection re-establishment • Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015, 3020, 3030, 3060, and 3080 models)

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Management	
Configuration	• Embedded management interface is accessible through console port, Telnet, SSHv1, and HTTPS • Administrator access is configurable for five levels of authorization; authentication can be performed externally through TACACS+ • Role-based management policy separates functions for service provider and end-user management • Monitoring • Event logging and notification through e-mail (SMTP) • Automatic FTP backup of event logs • Simple Network Management Protocol (SNMP) MIB-II support • Configurable SNMP traps • Syslog output • System status • Session data (including client assign IP, encryption type connection duration, client OS, and client version) • General statistics
Security	
Authentication and Accounting Servers	• Support for redundant external authentication servers, including: - RADIUS - Kerberos/Active Directory authentication - Microsoft NT Domain authentication - Microsoft NT Domain authentication with password expiration (MSCHAPv2); IPsec only
RSA Security Dynamics (SecurID Ready), Including Native Support for RSA 5 (Load Balancing, Resiliency)	• User authorization through Lightweight Directory Access Protocol (LDAP) or RADIUS • Internal authentication server for up to 100 users • X.509v3 digital certificates, including certificate revocation list (CRL)/LDAP and CRL/HTTP, CRL caching, and backup CRL distribution point support • RADIUS accounting • TACACS+ administrative user authentication
Internet-Based Packet Filtering	• Source and destination IP address • Port and protocol type • Fragment protection • FTP session filtering • Site-to-site filters and NAT (for overlapping address space)
Policy Management	• By individual user or group - Filter profiles (defined internally or externally) - Idle and maximum session timeouts - Time and day access control - Tunneling protocol and security authorization profiles - IP pool and servers - Authentication pool and servers
Certification	Federal Information Processing Standards (FIPS) 140-2 Level 2 (3.6), FIPS 140-1 Level 2 (3.1), and VPNC

Ports

Console port: asynchronous serial (DB-9)

Tables 7 and 8 list physical characteristics and power requirements for Cisco VPN 3000 Series Concentrators.

Table 7. Physical Characteristics

Concentrator	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3020	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Height	1.75 in. (4.45 cm)	3.5 in. (8.89 cm)	3.5 in. (8.89 cm)	3.5 in. (8.89 cm)	3.5 in. (8.89 cm)	3.5 in. (8.89 cm)
Width	17.5 in. (44.45 cm)	17.5 in. (4.45 cm)	17.5 in. (4.45 cm)	17.5 in. (4.45 cm)	17.5 in. (4.45 cm)	17.5 in. (4.45 cm)
Depth	11.5 in. (29.21 cm)	11.5 in. (29.21 cm)	11.5 in. (29.21 cm)	11.5 in. (29.21 cm)	11.5 in. (29.21 cm)	11.5 in. (29.21 cm)
Unit without front bezel or SEPS/PS	–	15 in. (38.1 cm)	15 in. (38.1 cm)	15 in. (38.1 cm)	15 in. (38.1 cm)	15 in. (38.1 cm)
Unit with front bezel, no SEPS/PS	–	16.19 in. (41.12 cm)	16.19 in. (41.12 cm)	16.19 in. (41.12 cm)	16.19 in. (41.12 cm)	16.19 in. (41.12 cm)

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Unit with front bezel and SEPS/PS	–	16.75 in. (42.55 cm)	16.75 in. (42.55 cm)	16.75 in. (42.55 cm)	16.75 in. (42.55 cm)	16.75 in. (42.55 cm)
Weight	8.5 lb (3.9 kg)	27 lb (12.3 kg)	28 lb (12.7 kg)	28 lb (12.7 kg)	33 lb (15 kg)	33 lb (15 kg)

Table 8. Power Type and Requirements

Concentrator	Cisco VPN 3005	Cisco VPN 3015, 3020, 3030, 3060, and 3080
Nominal	15W (51.22 BTU/hr)	35W (119.50 BTU/hr)
Maximum	25W (85.36 BTU/hr)	50W (170.72 BTU/hr)
Input Voltage	100 to 240 VAC	100 to 240 VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

Environmental

- Operating temperature: 32 to 131°F (0 to 55°C)
- Non-operating temperature: –4 to 176°F (–40 to 70°C)
- Humidity: 0 to 95 percent, non-condensing

Regulatory Compliance

- CE Marking

Safety

- UL 1950, CSA

EMC

- FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN50082-1, AS/NZS 3548 Class A, VCCI Class A

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Printed in USA C78-375540-00 10/06

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.